

CVE-2025-59689

Libraesva Email Security Gateway Command Injection Vulnerability

CISA KEV since Sep 29, 2025

Actively exploited

Libraesva ESG 4.5 through 5.5.x before 5.5.7 allows command injection via a compressed e-mail attachment. For ESG 5.0 a fix has been released in 5.0.31. For ESG 5.1 a fix has been released in 5.1.20. For ESG 5.2 a fix has been released in 5.2.31. For ESG 5.4 a fix has been released in 5.4.8. For ESG 5.5, a fix has been released in 5.5.7.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 6.1 Medium · NVD	EPSS 0.019 79.1st percentile · FIRST	CISA DEADLINE Oct 20, 2025 KEV since 2025 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.019 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
email security gateway	$\geq 4.5 < 5.0.31$ $\geq 5.1.0 < 5.1.20$ $\geq 5.2.0 < 5.2.31$ $\geq 5.3.0 < 5.3.16$ $\geq 5.4.0 < 5.4.8$ $\geq 5.5.0 < 5.5.7$	5.0.31 · 5.1.20 · 5.2.31 · 5.3.16 · 5.4.8 · 5.5.7	NVD

Sources

Vendor guidance	docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/	NVD	nvd.nist.gov/vuln/detail/CVE-2025-59689
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-30249
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-59689		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.